



DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID DoD-2021-OS-0128]

Privacy Act of 1974; System of Records

AGENCY: Department of Defense (DoD).

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the DoD proposes to establish a new Department-wide system of records titled, “Freedom of Information Act and Privacy Act Records,” DoD-0008. This system of records covers DoD’s maintenance of records about individuals who submit access requests and administrative appeals under the Freedom of Information Act, and who submit access and amendment requests and administrative appeals under the Privacy Act. This system of records data includes information regarding the individual requesters and their attorneys or representatives, the original request for access and any administrative appeal, and other supporting documentation to include related memoranda, correspondence, notes, and, in some instances, copies of requested records and records under administrative appeal. Additionally, DoD is issuing a Notice of Proposed Rulemaking, which proposes to exempt this system of records from certain provisions of the Privacy Act, elsewhere in today’s issue of the *Federal Register*.

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The Routine Uses are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* Federal Rulemaking Portal: <https://www.regulations.gov>. Follow the instructions for

submitting comments.

* Mail: DoD cannot receive written comments at this time due to the COVID-19 pandemic.

Comments should be sent electronically to the docket listed above.

Instructions: All submissions received must include the agency name and docket number for this *Federal Register* document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <https://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Rahwa Keleta, Defense Privacy, Civil Liberties, and FOIA Directorate, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Department of Defense, 1155 Defense Pentagon, Washington DC 20301-1155, OSD.DPCLTD@mail.mil; (703) 571-0070.

SUPPLEMENTARY INFORMATION:

I. Background

DoD is establishing the “Freedom of Information Act and Privacy Act Records” system of records as a DoD-wide Privacy Act system of records. A DoD-wide system of records notice (SORN) supports multiple DoD paper or electronic recordkeeping systems operated by more than one DoD component that maintain the same kind of information about individuals for the same purpose. Establishment of DoD-wide SORNs help DoD standardize the rules governing the collection, maintenance, use, and sharing of personal information in key areas across the enterprise. DoD-wide SORNs also reduce duplicative and overlapping SORNs published by separate DoD components. The creation of DoD-wide SORNs is expected to make locating relevant SORNs easier for DoD personnel and the public, and create efficiencies in the operation of the DoD privacy program.

This system of records concerns access requests and administrative appeals under the Freedom of Information Act (FOIA), and access and amendment requests and administrative

appeals under the Privacy Act. The system consists of both electronic and paper records and will be used by DoD components and offices to maintain records about individuals who submit FOIA access requests, Privacy Act access and amendment requests, administrative appeals to the Department under either the FOIA or Privacy Act, and FOIA and Privacy Act requests referred to DoD by other agencies. These records may include information regarding the individual requesters and their attorneys or representatives, the original request for access, amendment, or administrative appeal, and other supporting documentation to include related memoranda, correspondence, notes, statements of disagreement, and, in some instances, copies of requested records and records under administrative appeal.

Additionally, DoD is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in today's issue of the *Federal Register*. DoD SORNs have been published in the *Federal Register* and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties, and Transparency Division website at <https://dpcl.d.defense.gov>.

II. Privacy Act

Under the Privacy Act, a "system of records" is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A-108, DoD has provided a report of this system of records to the OMB and to Congress.

Dated: December 16, 2021.

Aaron T. Siegel,
Alternate OSD Federal Register

SYSTEM NAME AND NUMBER: Freedom of Information Act and Privacy Act Records (FOIA/PA Records) DoD-0008.

SECURITY CLASSIFICATION: Unclassified; Classified

SYSTEM LOCATION: Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, DC 20301-1000, and other Department installations, offices, or mission locations. Information may also be stored within a government-certified cloud, implemented and overseen by the Department's Chief Information Officer (CIO), 6000 Defense Pentagon, Washington, DC 20301-6000.

SYSTEM MANAGER(S):

A. Chief, Defense Privacy, Civil Liberties, and Transparency Division, Office of the Director of Administration and Management, 4800 Mark Center Drive, Mailbox #24, Alexandria, VA 22350-1700; OSD.DPCLTD@mail.mil; phone (703) 571-0070.

B. The contact information for the DoD Component FOIA Offices is found on the FOIA.gov website. The contact information for individual DoD Component Privacy Offices is found at this website: <https://dpclld.defense.gov/Privacy/Privacy-Contacts/>.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 113, Secretary of Defense; 5 U.S.C. 552, Freedom of Information Act, as amended; 5 U.S.C. 552a, Privacy Act of 1974, as amended; 32 CFR part 286, DoD Freedom of Information Act (FOIA) Program; 32 CFR part 310, Protection of Privacy and Access and Amendment of Individual Records Under the Privacy Act of 1974; DoD Directive, 5400.07, DoD Freedom of Information Act (FOIA) Program; DoD Instruction 5400.11, DoD Privacy and Civil Liberties Programs; DoD Manual 5400.07, DoD Freedom of Information Act (FOIA) Program; DoD 5400.11-R, DoD Privacy Program; and Executive Order 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM:

A. To report, track, and process access requests and administrative appeals under the FOIA, and access and amendment requests and administrative appeals under the Privacy Act.

B. To participate in and support litigation that may arise from a FOIA and/or Privacy Act access request, amendment request, or administrative appeal.

C. To assist DoD in carrying out any other responsibilities under the FOIA or the access or amendment provisions of the Privacy Act.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: (a) Individuals who submit access requests and appeals to the DoD for records under the provisions of the FOIA and the Privacy Act; (b) individuals who submit access requests to other Federal agencies whose requests have been referred to the DoD for processing or consultation; (c) individuals who request amendment of their records in a DoD system of records under the provisions of the Privacy Act and related appeals; and (d) attorneys or other representatives of the individuals listed above who carry out all or some of these activities on the individuals' behalf.

CATEGORIES OF RECORDS IN THE SYSTEM: Records created or compiled in response to FOIA access and Privacy Act access and amendment requests, and administrative appeals, including:

A. Original requests and administrative appeals (including requester's name, mailing address, case number, date and subject of the request, with some requesters also voluntarily submitting additional information such as SSNs, telephone numbers, e-mail addresses, and other identifying information) and responses to such requests and administrative appeals.

B. Correspondence with the individuals or entities that submitted the requested records and copies of the requested records, including records that might contain confidential business information or personal information.

C. Intra or interagency memoranda, referrals, correspondence, notes, fee schedules, assessments, cost calculations, and other documentation related to the processing of the FOIA and/or Privacy Act request or appeal.

D. Correspondence related to fee determinations and collection of fees owed under the FOIA or Privacy Act.

E. All related memoranda, correspondence, notes, statements of disagreement following a denial of an appeal of a Privacy Act record amendment request, and other related or supporting documentation;

F. Records concerning lawsuits brought under the FOIA and the Privacy Act including those obtained from the Department of Justice (DOJ) and other government attorneys; and

G. Types of personal information in the records may include: (1) requesters' and their attorneys' or representatives' identifying and contact information, such as name, address, email, telephone numbers, facsimile numbers, and FOIA/PA case numbers; (2) names and other identifying, descriptive, or contextual information about the individual(s) who is the subject of the request(s); (3) fee category, payment or non-payment information; (4) explanations or justifications provided in support of amendment requests, including supporting documentation;

(5) other identifiers that may be provided by or on behalf of a requester or appellant, such as Social Security number (SSN), driver's license number, DoD ID Number (EDI-PI), or other DoD-assigned number.

H. In some instances, copies of the requested records, if any; records subject to an amendment request; or such records when reviewed under administrative appeal. NOTE: Depending on the nature of the records subject to the appeal request, these may not be "records" under the Privacy Act or alternatively, may be covered by a separate system of records.

Note 1: This System of Records may contain individually identifiable health information. DoD Instruction 6025.18 and DoD Manual 6025.18 or any successor DoD issuances issued pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 45 CFR Parts 160 and 164, Health and Human Services, General Administrative Requirements and Security and Privacy, respectively, apply to most such health information. DoD Manual 6025.18 or a successor issuance may place additional procedural requirements on the uses and disclosures of such information beyond those found in the Privacy Act of 1974, as amended, or mentioned in this System of Records Notice (SORN).

Note 2: Individuals who file access or amendment requests may provide their SSN unsolicited to DoD within their request or appeal, or other materials they provide related to their request. In some cases, DoD may request an SSN to properly search for a record subject to a request for access or amendment if the SSN is a unique identifier used to retrieve information from that system of records.

Note 3: In general, this system of records will not be deemed to cover the underlying records that are responsive to an access or amendment request or administrative appeal. Rather, this system of records covers initial access and amendment requests and administrative appeals; all related correspondence, notes, and memoranda created as a result of such requests and appeals; and the other categories of records itemized in paragraphs (A) – (G). In the case of a first-party

Privacy Act request, underlying responsive records will typically be covered by a separate system of records.

RECORD SOURCE CATEGORIES:

A. Individuals who submit initial access requests and administrative appeals pursuant to the FOIA and individuals submitting access or amendment requests and administrative appeals under the Privacy Act;

B. DoD personnel assigned to handle such requests and appeals, or related litigation arising therefrom;

C. Other agencies that have referred to DoD requests or consultations concerning DoD records or who have consulted with DOJ regarding the handling of an access or amendment request; and

D. Submitters of or subjects of information reflected in records subject to access requests that have provided assistance to the DoD in making access or amendment determinations.

In addition, copies of records subject to the access or amendment request are obtained from agency systems of records and/or other paper and electronic record-keeping systems containing records searched or otherwise relevant to such requests.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as a Routine Use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.

B. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction

with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

C. To any component of the DOJ for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

H. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems,

programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

I. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

J. To the NARA, Office of Government Information Services (OGIS), to the extent necessary to fulfill its responsibilities in 5 U.S.C. 552(h), to review administrative agency policies, procedures and compliance with the FOIA, and to facilitate OGIS's offering of mediation services to resolve disputes between persons making FOIA requests and administrative agencies.

K. To a Federal agency or other Federal entity that furnished the record or information for the purpose of permitting that agency or entity to make a decision regarding access to or correction of the record or information, or to a Federal agency or entity for purposes of providing guidance or advice regarding the handling of particular requests.

L. To the DOJ, to the Department of the Treasury, or to a consumer reporting agency for collection action on any delinquent debt when circumstances warrant.

M. To the Office of Management and Budget (OMB) or the DOJ to obtain advice regarding statutory and other requirements under the FOIA or Privacy Act.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records may be stored locally on digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by full name of requestor; FOIA or Privacy Act case number or appeal number; date and/or year of request or appeal; subject matter; and in some instances may be retrieved by other identifiers assigned by the component.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Retention and disposal of records in this system of records is governed by General Records Schedule 4.2, Information Access and Protection Records, as follows:

A. *Access request files.* Case files created in response to requests for records under the FOIA and Privacy Act, including administrative appeals, are destroyed six years after final agency action (initial response or appeal) or three years after final adjudication by the courts if applicable, whichever is later. (Note: National Security Agency documents and supporting files created in response to FOIA requests and appeals are destroyed when 50 years old.)

B. *Privacy Act amendment request files.* Files relating to an individual's request to amend a record subject to the Privacy Act and any appeal or civil action that follows are destroyed with the records for which amendment was requested or four years after the final determination by agency or final adjudication by the courts if applicable, whichever is later.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; Secret Internet Protocol Router (SIPR) token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have

access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should follow the procedures in 32 CFR part 310. Individuals should address written inquiries to the DoD office with oversight of the records. The public may identify the contact information for the appropriate DoD office through the following website: www.FOIA.gov. Signed written requests should contain the name and number of this system of records notice along with the full name, current address, email address, and telephone number of the individual. The individual should also include the FOIA or Privacy Act case identification number, if available. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate format:

If executed outside the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).”

If executed within the United States, its territories, possessions, or commonwealths: “I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).”

Note 4: In general, this system of records will not be deemed to cover the underlying records that are responsive to an access or amendment request. Rather, this system of records covers the access, amendment, or appeal requests themselves, correspondence created as a result of such requests, and the other categories of records itemized in paragraphs (A) – (G) of the Categories of Records section. In the case of a first-party Privacy Act request, underlying responsive records will typically be covered by a separate system of records. Consistent with paragraph (H)

in the Categories of Records section, this system of records does not confer to a FOIA requester access rights under the Privacy Act to copies of the requested records.

CONTESTING RECORD PROCEDURES: Individuals seeking to amend or correct the content of records about them should follow the procedures in 32 CFR part 310.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Records Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: Pursuant to 5 U.S.C. 552a(j)(2), portions of this system are exempt from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g). Additionally, pursuant to 5 U.S.C. 552a(k)(1), (k)(2), (k)(3), (k)(5), (k)(6), and (k)(7) portions of this system are exempt from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). When DoD is processing Privacy Act and/or FOIA requests, responding to appeals, or participating in FOIA or Privacy Act litigation, exempt materials from other systems of record may become part of the records in this system. When exempt records received from other systems of records become part of this system, DoD also claims the same exemptions for those records that are claimed for the prior system(s) of records from which they originated and claims any additional exemptions set forth here. Exemption rules for this system have been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c), and (e) and published in 32 CFR part 310.

HISTORY: None.